MEDDAC/DENTAC Regulation 190-2

Military Police

Physical Security Plan

Headquarters
U.S. Army Medical Department Activity
Fort George G. Meade
2480 Llewellyn Avenue
Fort George G. Meade, MD 20755-5800
25 June 2003

Unclassified

SUMMARY of CHANGE

MEDDAC REG 190-2
Physical Security Plan

Specifically, this revision—

- Has been published in a new format that includes a cover and this "Summary of Change" page.

- Reformats the title page. The Contents section now includes the page numbers that the various chapters and paragraphs begin on.

- Institutes using the term "administrative officer of the day (AOD)" to also represent the similar functions of staff duty, charge of quarters, and like functions, as utilized at the various MTFs belonging to the MEDDAC.

- Makes other minor changes throughout the regulation.

Department of the Army
Headquarters
United States Army Medical Department Activity
2480 Llewellyn Avenue
Fort George G. Meade, Maryland 20755-5800
25 June 2003

*** MEDDAC/DENTAC Regulation 190-2**

Military Police

Physical Security Plan

FOR THE COMMANDER:

PATRICK J. SAUER
LTC, MS
Deputy Commander for Administration

PATRICE E. GREENE
COL, DE
Commanding

Official:

JOHN SCHNEIDER
Adjutant

History. This is the second revision of this publication, which was originally published on 24 March 1999.

Summary. This regulation establishes policies and procedures for the safeguarding of personnel, materials and facilities, and to prevent unauthorized access to equipment, material and documents within the medical treatment facilities (MTFs) of the U.S. Army Medical Department Activity, Fort George G. Meade (MEDDAC).

Applicability. This regulation applies to the MEDDAC headquarters (that is, Kimbrough Ambulatory Care Center (KACC)), all outlying clinics, and Dental Clinic No. 3 (DC#3), U.S. Army Dental Activity, Fort George G. Meade (DENTAC).

Proponent. The proponent of this regulation is the Chief, Plans, Training, Mobilization and Security Division (PTM&S).

Supplementation. Supplementation of this regulation is prohibited.

Suggested improvements. Users of this publication are invited to send comments and suggested improvements, by memorandum, directly to the Commander, U.S. Army Medical Department Activity, ATTN: MCXR-PTMS, Fort George G. Meade, MD 20755-5800, or to the MEDDAC's Command Editor by fax to (301) 677-8088 or e-mail to john.schneider@na.amedd.army.mil.

Distribution. Distribution of this publication is made by electronic medium only.

Contents (Listed by paragraph and page number)

* This publication supersedes MEDDAC Reg 190-2, dated 12 September 2001.

Contents–continued

Contents–continued

Chapter 1
Introduction

1-1. Purpose
This regulation establishes responsibilities, policies, and procedures for the safeguarding of personnel, material and facilities, and to prevent unauthorized access to equipment, material and documents within the facilities of the MEDDAC.

1-2. References
Required and related publications are listed in appendix A. Referenced forms are also listed in appendix A.

1-3. Explanation of abbreviations
Abbreviations used in this regulation are explained in the glossary.

1-4. Use of pronouns in this regulation
The pronouns he, his, him and himself include she, hers, her and herself.

Chapter 2
Responsibilities

2-1. The MEDDAC Commander
The MEDDAC Commander is responsible for the overall Physical Security Program and will designate, on orders, a MEDDAC Physical Security Officer (PSO), which may be a noncommissioned officer (NCO), to assist in implementation of this program and to supervise the day-to-day activities of physical security. Normally, the PSO will be on the staff of the Plans, Training, Mobilization and Security Division (PTM&S).

2-2. The Chief, PTM&S
The Chief, PTM&S will correct security-related deficiencies, such as burned out security lights and faulty locks, on a priority basis.

2-3. The Medical Company First Sergeant (1SG) and detachment NCOs
a. The Medical Company 1SG will—

(1) Ensure that the information concerning administrative officer of the day (AOD) operations in paras 3-5 and 3-6, below, is included in the MEDDAC's AOD Instructions book.

(2) Report deficiencies in security lighting, as noted by AOD personnel, to the Chief, PTM&S. (See paragraph 3-6c, below.)

b. Detachment NCOs at the outlying clinics will follow the guidance in their medical treatment facility's (MTF's) physical security plan.

2-4. The PSO
The PSO will—

a. Advise the MEDDAC Commander on all matters pertaining to the physical security and crime prevention programs.

b. Be the liaison with Fort George G. Meade law enforcement and security elements. Coordinate outside security organizations' physical security surveys and inspections of KACC.

c. Enforce procedures and standards for physical security and crime prevention within KACC.

d. Conduct physical security inspections of activities at KACC. (The term "activity" is explained in the glossary.)

e. Investigate reported security incidents and failures at KACC.

f. Maintain a list of activities at KACC and other MEDDAC MTFs that require annual physical security surveys and inspections.

g. Quarterly, report the status of the MEDDAC Physical Security Program to the Safety and Environment of Care Committee.

h. Coordinate and supervise security operations for all organizational functions requiring an increased level of security.

i. Ensure education is provided to staff concerning physical security.

2-5. Outlying clinic security managers (SMs)

Outlying clinic SMs will—

a. Enforce procedures and standards for physical security and crime prevention within their MTFs.

b. Educate their facilities on security and crime prevention techniques.

c. Quarterly, report the status of the MTF's security programs to the PSO.

2-6. Activity physical security representatives

Activity physical security representatives are normally NCOs; however, a civilian may be designated to perform this duty if an NCO is not available. Physical security representatives will—

a. Prepare a physical security standing operating procedure (SOP) to support their activity. A sample SOP is at appendix B. Provide a copy of the SOP to the PSO/SM.

b. Train the activity's personnel on security topics as directed by the PSO/SM.

2-7. All employees

All employees will be alert for items that are missing, out of place, or are foreign to the area. (The term "employee" is explained in the glossary.) All employees are authorized to conduct spot checks of suspicious appearing personnel or acts at any time. These checks will be made to reduce and discourage entry of unauthorized personnel to sensitive and restricted areas, and to provide adequate visitor identification. MEDDAC employees will not conduct searches of other persons. All searches will be conducted by the military police (MPs). Questions regarding the validity of conducting spot checks will be addressed to the PSO/SM.

Chapter 3
Access to MTFs

3-1. General

The procedures in this chapter pertain specifically to KACC. SMs at the outlying clinics will develop similar procedures for their MTFs and will include these procedures in their MTF's physical security plans.

3-2. Use of security identification (ID) badges at KACC

MEDDAC Memo 190-1 outlines the procedures for the issuance, accountability, turn-in, and disposition of security ID badges at KACC. Paragraph 2-5 of that memorandum addresses enforcement procedures regarding the discovery of personnel without valid ID badges.

3-3. Visitor control during duty hours

Within each activity at KACC, visitor control during duty hours is the responsibility of the officer in charge (OIC) or NCO in charge (NCOIC). (The term "duty hours" is explained in the glossary.)

3-4. Visitor control during non-duty hours

During non-duty hours, visitors whose destination is a clinic or other activity that is open on extended hours, such as the After Hours Clinic (AHC) or the Pharmacy, will be allowed to proceed to those activities. All other visitors will be directed to the AOD Desk for assistance.

3-5. Emergency vehicle access to KACC

Except for authorized emergency medical vehicles, blocking access to the AHC is prohibited. Unauthorized vehicles blocking access to the AHC will be resolved as follows by the AHC OIC, or his designated representative:

a. Contact the Information/AOD Desk (78392). Give a description of the vehicle, to include the state and number of the license plate, and ask the individual on duty at the desk to announce that the vehicle must be removed immediately by the owner because it is blocking the emergency vehicles entrance adjacent to the Occupational Health Environmental Safety Service (OHESS) Clinic, and that if it is not removed, the MPs will be called and it will be towed away at the owner's expense.

b. If the owner has not removed the vehicle within 10 minutes, call the Military Police (MP) Desk Sergeant (76622/3) and ask him to have the vehicle towed.

3-6. The AOD and physical security

During non-duty hours, the AOD will conduct security checks of controlled areas and security lighting and note these checks on DA Form 1594 (Daily Staff Journal or Duty Officer's Log) to include the following:

a. A physical examination of windows and doors for evidence of forcible entry. Call the MPs if an illegal entry or security incident has occurred or is suspected.

b. A test of the entry door (door rattle) to ensure entry way is properly secured. Call the MPs if an illegal entry or security incident has occurred or is suspected.

c. Security lighting will be checked for operation. The Medical Company First Sergeant will inform the Chief, PTM&S of any security lighting deficiencies noted on DA Form 1594.

3-7. Intrusion detection systems (IDSs)

a. Activities having controlled areas will conduct daily checks of their IDS and associated daily security checks as follows.

(1) The IDS will be checked for operation by personnel assigned to controlled areas, in accordance with (IAW) AR 190-51. The PSO will be notified of malfunctions immediately.

(2) The activity's chief, OIC or NCOIC will annotate checks of the IDS on DA Form 4930-R (Alarm/Intrusion Detection Record).

(3) Activated IDS alarms will be handled by responding MPs. The activity chief, OIC or

NCOIC will immediately notify the PSO if the IDS alarm sounds.

3-8. Testing of duress alarm systems

Duress Alarm Systems will be tested semiannually to ensure proper operation. The PSO will coordinate with the appropriate department or division supervisor and the installation Provost Marshal for scheduling of this test.

3-9. Theft, loss, mismanagement, and recovery of controlled substances and sensitive items

Theft, loss, mismanagement and recovery of controlled medical substances or other medical substances or other medically sensitive items will be reported on a serious incident report, IAW AR 190-40, with U.S. Army Medical Command Supplement 1.

Chapter 4
Security and Accountability of Security Containers Used for Storing Classified Information

4-1. General

a. The security and accountability of security containers, secure rooms and vaults will depend upon the material protected by the security container. (Throughout this chapter, the term "security container" will also represent secure rooms and vaults.)

b. A security container will not be used to store more than one classification of material. There are two classes of material:

(1) Classified material.

(2) Controlled substances and medically sensitive items, including operational quantities of precious metals, needles and syringes.

c. Any security container (safe or filing cabinet) which weighs less than 750 pounds will be secured to the building by a chain and padlock. The chain will be a gauge no smaller than the shackle of the padlock and will be of hardened steel with closed links. A medium padlock, also constructed of hardened steel, is adequate for this purpose. Do not use brass "arms room" locks as these can be easily twisted open with the handle of a pliers or large screwdriver.

4-2. Security containers used for storing classified material

a. Classified material will be secured only in security containers that meet Government Supply Agency (GSA) requirements for storage of classified material. Standards for storage of material may be found in AR 380-5, chapter V. Within the MEDDAC, only GSA approved security containers with internal combination locks will be used to secure classified material unless prior coordination is made with the Installation Security Manager.

b. Combinations will be changed only by individuals who possess the proper security clearance. Combinations will be changed—

(1) When a security container is initially placed in use.

(2) When an individual with knowledge of the combination departs the activity, or otherwise no longer has a need to access the contents of the security container.

(3) When the combination has been subject to possible compromise.

(4) Annually.

c. A security container's combination will be assigned a security classification equal to the

highest classification of material stored therein.

d. Standard Form (SF) 700 (Security Container Information) will be maintained for each security container used for storing classified information. The names, home addresses and home telephone numbers of all personnel having knowledge of the combination will be entered on the SF 700.

e. SF 702 (Security Container Check Sheet) will be used to record each opening and closing of security containers. If a security container is not opened during a 24-hour period; i.e., between 0001 and 2400 on the same day, at least one security check of the container must be accomplished during that period and must be reflected on the security container's SF 702. The SF 702 will be maintained at least 24 hours after the last entry before it is destroyed.

f. Combinations to security containers containing classified information will be disseminated to as few personnel as mission requirements permit. Only personnel who are authorized access to information in a security container will be given its combination.

g. The number of security containers used for storing classified material will be kept to an absolute minimum consistent with mission requirements.

h. Electronic push button (or cipher locks) will not be used to protect classified material.

4-3. Security containers used to store controlled substances, medically sensitive items, and other material

This paragraph does not apply to the storage of classified information. For information concerning the storage of classified information, see paragraph 4-1, above. Nor does this paragraph apply to safes secured by key type locks. These keys will be controlled IAW MEDDAC Reg 190-1.

b. SF 702 will be used and affixed to the outside of the security container. The form will be marked in bold letters, "THIS DOES NOT CONTAIN CLASSIFIED INFORMATION."

c. SF 702 will be used to record times of opening, closing and security checks. The form will be retained for 90 days from the date of the last entry, after which time it will be destroyed unless it is needed for an investigation.

d. Combinations will be recorded on SF 700, which will be stored in the PSO's security container. All combination records will be marked and protected as "FOR OFFICIAL USE ONLY."

e. Combinations will be changed IAW paragraph 4-2b, above.

Chapter 5
Safeguarding Purses and Wallets and Government Property, Reporting Thefts, Reporting and Investigating Security Incidents, Very Important Persons (VIPs), and Civil Disturbances

5-1. Safeguarding purses and wallets

Purses and wallets brought to work are the responsibility of the owner. If not maintained on your person, your wallet or purse should be secured during normal duty hours in a lockable container. See your supervisor if you do not have a lockable container.

5-2. Safeguarding Government property

The MEDDAC uses AR 190-51 as guidance for the safeguarding of Government property.

5-3. Reporting thefts

a. All thefts occurring to staff members and patients will be reported as follows by the staff

member to whom the theft occurred or on behalf of a patient to whom the theft occurred by a member of the staff:

(1) The staff member must report the theft to the following officials:

(a) The immediate supervisor or department or division NCOIC.

(b) The PSO/SM.

(2) In addition, the staff member may report the theft to the MPs himself, even if the PSO/SM has stated that he will report it to the MPs.

b. After receiving the report of a theft, the PSO/SM will notify—

(1) The MPs, if warranted.

(2) Logistics Division, if Government property has been stolen.

5-4. Reporting security incidents and failures

A security incident is any incident that endangers patients, visitors, employees or property of the organization. Report security incidents as follows:

a. During normal duty hours, immediately to the PSO/SM.

b. During non-duty hours, to the AOD, staff duty, charge of quarters (or other individual as designated by the MTF commander for MTFs that do not have an AOD, staff duty or charge of quarters function). (From this point forward, "AOD" will also represent the terms "SD," "CQ," and "other designated individual.") The AOD will notify the PSO/SM or the commander if the incident is so serious that it cannot wait until the next duty day or cannot be corrected on the spot. (The term "commander" is explained in the glossary.)

5-5. Investigating security incidents

Security incidents will be investigated immediately by the PSO/SM. Appropriate action will be taken to correct the problem and preclude similar incidents in the future.

5-6. Civil disturbances

A civil disturbance is any interference to the normal operations of the MTF that involves non-employees. Report civil disturbances as follows:

a. During normal duty hours, immediately to the PSO/SM. The PSO/SM will investigate and take appropriate action or contact appropriate outside agencies for assistance.

b. During non-duty hours, to the AOD. If law enforcement assistance is needed, the AOD will immediately notify the MPs. If the MPs are notified, the MTF commander will be notified immediately after the MPs have been called.

5-7. Very important persons (VIPs)

This procedures included in this paragraph pertain specifically to KACC. SMs at the outlying clinics will develop similar procedures for their MTFs and will include these procedures in their MTF's physical security plans.

a. Announced VIP visits. High ranking and other important visitors scheduled to visit the facility will be coordinated through the office of the Deputy Commander of Administration (DCA).

b. Unannounced visits of VIPs. Personnel who identify unescorted VIPs will immediately notify the DCA's office. The DCA will investigate and take appropriate action.

c. Security measures required for VIPs will be coordinated by or through the PSO.

Chapter 6
Interacting with the Media

6-1. General
Guidance for interacting with the media (newspapers, magazines, radio and television) is provided in AR 360-1. It is normally the public affairs officer's (PAO's) responsibility to contact the media and invite them to the installation, to provide them with telephonic interviews and or to arrange such interviews with members of the staff, and to fax news releases to them.

6-2. Who may interact with the media
a. Interacting with the media is normally a responsibility of the MTF's PAO.

b. At the MEDDAC headquarters, the MEDDAC Commander, DCCS, DCA, DCN and Senior Medical NCO, as primary members of the command group, are authorized to interact directly with the media. These individuals may interact directly with the media in the absence of the PAO, or whenever it is deemed necessary because of the situation.

c. Outlying clinics that have PAOs will follow the guidance in para b.

d. All other outlying clinics must utilize someone on the headquarters staff to interact with the media.

6-3. Obtaining PAO assistance to interact with the media
Any PAO or member of an MTF headquarters staff who needs guidance or assistance in dealing with the media may contact his installation PAO and or the MEDDAC PAO. In extreme situations when the installation and or MEDDAC PAO are not available to assist in the matter, the MTF should contact the Walter Reed Army Medical Center PAO at (202) 782-7177.

6-4. Inviting members of the media to the MTF or installation
Only the installation PAO, unit PAO, commander or member of the commander's primary staff is authorized to invite members of the media (reporters) to the MTF or anywhere else on the installation. If members of the media are invited onto the installation by the MTF's PAO, commander or member of the commander's primary staff, a courtesy call will be made to the installation PAO to inform them that the media has been invited onto the installation, the identity(ies) of the media, the subject of the visit, when they are expected to arrive and leave, and where they will be on the installation. Installation commanders and PAOs like to know when and why the media is on their installations. They do not like to discover this on their own or learn about it after the fact.

6-5. Making statements to members of the media
a. Whenever possible, statements made to members of the media regarding subjects covered by this regulation will be cleared by the MTF commander or a member of the commander's primary staff, who will either pass it to the MTF's PAO or take some other action to deliver the statement to the media. There will be times when employees are questioned outright by reporters; this cannot be helped. In such situations, employees should remember the following:

(1) Reporters must be escorted by the MTF's PAO or some other member of the staff while in the MTF or on it's grounds. If you are approached by a reporter who is unescorted, do not say anything to the reporter. Notify the MTF PAO or commander's office that a member of the media is on the premises and ask for guidance.

(2) If it's not your job and or you have no special knowledge of the incident, make no

comment except to say that you are either not qualified or don't know. Do not make it appear that you are trying to conceal information. It is much better to make no comment at all than to make one that is not entirely factual.

(3) If it is your job and or you have special knowledge of the incident, it is alright to respond to the reporter's questions; however, think before you respond. An ill-chosen word or phrase, or even a gesture, can change the entire meaning of your response. Interviews that take minutes to make are reduced to mere seconds in the cutting rooms of television news rooms. Poorly chosen words and phrases can easily be taken out of context, resulting in a televised version of your interview that is contrary to what you actually stated.

b. Commanders of outlying clinics will inform the MEDDAC Commander of all statements made to the media by themselves, their primary staff and all other employees. The MEDDAC commander will be furnished a transcript of the verbal transaction between the reporter and interviewee, to be followed up, if possible, by a copy of the printed article or summary of the television newscast resulting from the interview.

c. The KACC PAO will designate a holding area for media representatives during a disaster or serious event.

6-6. Rights of employees regarding interaction with members of the media

a. What employees may not do. Except for those officials specified in para 6-4 above, MEDDAC employees may not—

(1) Invite a member of the media onto an Army installation.

(2) Offer to be interviewed by the media or offer a response to a question from the media, while on duty, without first being authorized to do so by his supervisor.

b. What employees may do. All MEDDAC employees may—

(1) Arrange to be interviewed by the media, or respond to a question from the media, when not on duty and off the installation. Following are examples of what is and is not allowed:

(a) Example 1: An employee calls Channel X and invites a reporter to meet him at his off-post residence to be interviewed at his off-post residence, in the evening, after work. This is permissible because the employee is engaging in the interview off-post and on his own time.

(b) Example 2: An employee who lives on-post calls Channel X and invites a reporter to meet him at his on-post residence to be interviewed in the evening, after work. This is not permissible because the employee has invited the media onto the installation without the permission of the Post Commander.

c. Any employee who desires to initiate a meeting with the media is urged to express this desire to his commander instead of contacting the media directly. By doing this, the employee will give the commander an opportunity to provide an answer to the problem (if there is a problem) or to invite the media officially himself. At the very least, this will forewarn the commander that the interview will be forthcoming so that he will not be caught unawares after it is published or televised.

Chapter 7
Restricted and Sensitive Areas

7-1. Vulnerable mission-essential restricted and sensitive areas

The following areas are mission-essential and may be vulnerable to unauthorized or criminal

activities. Access to these areas during non-duty hours is limited to personnel assigned to them.

a. Restricted area. The Pharmacy is the only area designated as restricted access. Entry by non-Pharmacy personnel is not permitted except when escorted by someone on the Pharmacy's unaccompanied access roster.

b. Sensitive areas. The following list is comprised of activities at KACC; however, similar activities at outlying clinics are also deemed sensitive areas:

(1) Ambulatory Surgical Records.
(2) Credentials Office.
(3) Laboratory Service.
(4) Mailroom.
(5) Outpatient Medical Records.
(6) PTM&S.
(7) The Quality Management Office.
(8) All clinical areas.
(9) All areas belonging to Logistics Division.

7-2. Procedures for protecting restricted and sensitive storage areas, information and material

a. Classified information. Procedures for storage and safeguarding of classified information are contained in AR 380-5.

b. Narcotics and sensitive drugs. Procedures for storage and safeguarding of narcotics and sensitive drugs are contained in AR 190-51.

c. Patient trust funds and valuables. Procedures for care and safeguarding of patients' trust funds and valuables are contained in AR 40-2.

d. Equipment and supplies storage areas. Equipment (to include facilities) and supply areas will be protected by limiting access to personnel actually required by their duties to be in such areas and through the use of locks and or physical barriers. The Chief, PTM&S and appropriate activity chiefs will be responsible for authorizing entrance to those storage areas under their control. Normal supply inventory and property accountability procedures will be used to provide checks against theft and pilferage.

e. Unattended patient care areas. Patient care areas that are not attended after normal duty hours and are not routinely used during such hours will be locked. The activity OIC or NCOIC will be responsible for all such areas. Areas that cannot be locked due to usage or are incapable of being locked will have all unessential equipment removed to a secure area or locked in compartments or cabinets within the area. The AOD will incorporate checks of these areas into his security rounds.

f. Unattended work areas. Work areas that are not attended after normal duty hours and are not routinely used during such hours will be locked. The activity OIC or NCOIC will be responsible for checking the security of the work area and completing the SF 701.

g. Unattended buildings. Buildings that are not normally used either during normal or non-duty hours will be locked. Notification of the status of such buildings will be given to the Provost Marshal. Whenever possible, non-duty hour checks will be made of such buildings by the Provost Marshal's Office. Routine duty hour checks of such buildings will be made by personnel responsible for them.

h. Attended patient care areas and work areas. The assigned personnel of these areas will take those measures deemed necessary by the responsible activity chief to ensure adequate security

during normal duty hours. Activity personnel and the AOD or CQ are authorized to make spot checks of personnel to ensure that all personnel in those areas have a need or are authorized access to those areas. The activity OIC and or NCOIC will be responsible for checking the security of the work area and completing the SF 701.

i. Attended buildings. Buildings that are attended during normal duty and or off-duty hours will be secured by personnel in such buildings. The AOD or CQ and activity personnel will make periodic checks to ensure that all personnel in those areas have a need or are authorized access to those areas.

j. Grounds. Periodic non-duty hour checks of grounds and lighting will be made by the AOD or CQ as detailed in their AOD or CQ instructions.

Chapter 8
Carrying of firearms within the MEDDAC's MTFs

8-1. Who is authorized to carry firearms within the MEDDAC's MTF

Only on-duty MPs, Criminal Investigation Division (CID) agents, agents of federal law enforcement agencies, and civilian law enforcement personnel are authorized to carry firearms (weapons) within the MTFs. MP, CID agents, and civilian law enforcement personnel arriving at an MTF for emergency treatment with weapons will be treated, regardless of their duty status. Non-emergent situations will be treated as follows.

8-2. MPs

a. *When MPs are authorized to carry weapons into an MTF*. MPs are authorized to carry their issued weapons into an MTF if they are actually performing law enforcement duties.

(1) An MP Duty Officer or uniformed MP who is performing law enforcement duties will be wearing a uniform authorized by the local provost marshal and an MP brassard; i.e., a black arm band worn on the left arm, at the shoulder, with "MP" on it in large, white letters. His weapon will be worn in a holster, unconcealed.

(2) An MP investigator will be in plain clothes, will carry credentials identifying him as an MP investigator, and will be carrying a concealed weapon.

b. *When MPs are not authorized to carry weapons into an MTF*. MPs who are on duty but not actually engaged in law enforcement duties within the MTF are not authorized to carry their weapons into the MTF, as in the following examples. In such cases, the MP must return to his headquarters and check in his weapon before proceeding to the MTF.

(1) An MP who enters the MTF for his own medical or dental appointment.

(2) An MP who accompanies a family member on a medical or dental appointment.

8-3. CID agents

CID agents are authorized to carry their weapons at all times, regardless of their duty status. CID agents will always be in plain clothes and carry concealed weapons. Upon arrival at an MTF, regardless of the reason, a CID agent is required to state that he is a CID agent, present his CID identification, and indicate that he is carrying a concealed weapon.

8-4. Agents of federal law enforcement agencies

Agents of federal law enforcement agencies, such as the Federal Bureau of Investigation; Central

Intelligence Agency; Bureau of Alcohol, Tobacco and Firearms; and the Drug Enforcement Administration, are authorized to carry their firearms 24 hours per day, every day. Such agents should, upon arrival within the facility, state that they are an agent for such-and-such agency, and produce their agency identification for examination.

8-5. Civilian law enforcement officials

In rare instances, civilian law enforcement officials will enter an MTF on official business. Since these officials have no jurisdiction on federal installations, it is obligatory for them to present to the local MP station and state their reason for being on the installation. A civilian law enforcement official on official business within an MTF is authorized to carry his weapon.

8-6. What to do if someone presents with an unauthorized firearm

Only the personnel stated in paragraphs 8-1 through 8-5, above, are authorized to carry firearms within the MTF, and only under the conditions stated. In the case of any military and civilian law enforcement individual not complying with the above requirements, the incident should be brought to the attention of MTFs security officer immediately and the installation MP station. At KACC, contact the Physical Security Officer in PTM&S by calling 78697, 78699 or 78608, and the military police at 76673. An MP who presents for a medical or dental appointment for himself or a family member, and who is carrying a weapon, should be informed that he is in violation of the MTF's policy, and inform him that he cannot be treated or that he cannot be present while his dependent is being treated, until he has secured his weapon at the MP station. Do not enter into a confrontation with an individual who refuses to relinquish his weapon.

Appendix A
References

Section I
Required Publications

AR 40-2
Army Medical Treatment Facilities - General Administration. (Cited in para 7-2.)

AR 190-40
Serious Incident Report. (Cited in para 3-9.)

AR 190-51
Security of Unclassified Army Property. (Cited in paras 3-7 and 7-2.)

AR 380-5
Department of the Army Information Security Pro-gram. (Cited in para 7-2.)

MEDDAC Memo 190-1
Security Identification Badge System (SIBS). (Cited in para 3-2.)

MEDDAC Reg 190-1
Key and Lock Control. (Cited in para 4-3.)

Section II
Related Publications

AR 190-14
Carrying of Firearms and Use of Force for Law Enforcement and Security Duties

AR 360-1
The Army Public Affairs Program

Section III
Referenced Forms

DA Form 1594
Daily Staff Journal or Duty Officer's Log

DA Form 4930-R
Alarm/Intrusion Detection Record

SF 700
Security Container Information

SF 701
Activity Security Checklist

SF 702
Security Container Check Sheet

Appendix B
Sample Physical Security SOP

The activity's physical security SOP will be prepared on plain bond paper, utilizing the sample format below for general guidance. The SOP will be signed by the activity chief or OIC. If there is no chief or OIC, it will be signed by the NCOIC.

1. Purpose. To establish proper physical security policies and procedures for (name of activity).

2. Key Control.

    a. Key Custodian (designate by position).

    b. Policy governing issue of keys.

    c. Procedures for issue and retrieval of keys.

3. Access to areas. Policy governing identification and admittance during duty and non-duty hours.

4. Access to files

    a. Personnel, by position, who have access.

    b. Procedure for securing sensitive documents.

5. Control of supplies and equipment.

6. Lockup procedures. Identification of personnel, by position, who are responsible for the following at close of duty day:

    a. Security equipment.

    b. Disconnecting electrical equipment.

    c. Locking windows and doors.

7. Detection of losses. Describe the means by which missing supplies and equipment can be readily detected and identified.

8. Location of warning and non-intrusion signs; for example, "No Visitors," "Unauthorized Entry Prohibited," "No Trespassing," "Keep Out," "No Non-duty Entrance," "Door Locked (hours) to (hours)," "Fire Exit Only," "Exclusion Area," "Enter Only by Order of Commanding Officer," and "Unauthorized Entry Subject to Prosecution."

Glossary

Section I
Abbreviations

1SG
first sergeant

AHC
After Hours Clinic

AOD
administrative officer of the day

CID
Criminal Investigation Division

DCA
Deputy Commander for Administration

DC#3
Dental Clinic Number 3, DENTAC

DENTAC
U.S. Army Dental Activity, Fort George G. Meade

GSA
General Services Administration

IAW
in accordance with

ID
identification

KACC
Kimbrough Ambulatory Care Center

MEDDAC
U.S. Army Medical Department Activity, Fort George G. Meade

MP
military police

MTF
medical treatment facility

NCO
noncommissioned officer

NCOIC
NCO in charge

OIC
officer in charge

PAO
public affairs officer

PSO
physical security officer

PTM&S
Plans, Training, Mobilization & Security Division

SF
standard form

SM
security manager

VIP
very important person(s)

Section II
Terms

Activity
Any administrative office, clinic or other type of work area that has it's own military or civilian chief or OIC. In some activities, the highest ranking individual is the NCOIC.

Administrative officer of the day (AOD)
The individual designated by the MTF commander to be responsible for the MTF during non-duty hours. Within this regulation, the term AOD also represents the similar functions of staff duty and charge of quarters.

Commander
The individual in charge of the MTF; the commander, director, OIC or chief, as applicable. It also means any individual who is in an official acting capacity for the "commander."

Duty hours
The hours of operation of an individual activity; the daily duty hours of an individual.

Employee
All military personnel, regardless of service, and all civilians, to include contract civilians and providers, Red Cross volunteers and Veterans Affairs field representatives, who work at any of the MEDDAC's MTFs full-time or part-time.

Non-duty hours
Any period of time that does not fall within the definition of normal duty hours. (See the definition of "normal duty hours," below.)

Normal duty hours
Within KACC, normal duty hours are 0730 to 1600, Monday through Friday, except Federal holidays and training holidays. Commanders of outlying clinics may choose to specify other normal duty hours, as best befits the operations of their host installations.

Security container
Within this regulation, the term "security container" means safes and file cabinets that have been approved by the GSA for storage of classified material, vaults, and secure rooms.